CLAIMS

What is claimed is:

1. A method comprising:

determining at least one Squared Tate pairing for at least one hyperelliptic curve; and

cryptographically processing selected information based on said determined Squared Tate pairing.

2. The method as recited in Claim 1, wherein said Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K.

3. The method as recited in Claim 1, wherein determining said Squared Tate pairing further includes:

forming a mathematical chain for m, wherein m is a positive integer and an m-torsion element D is fixed on Jacobian of said hyperelliptic curve C.

4. The method as recited in Claim 3, wherein said mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain.

5. A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

calculating at least one Squared Tate pairing for at least one hyperelliptic curve; and

cryptographically processing selected information based on said determined Squared Tate pairing.

6. The computer-readable medium as recited in Claim 5, wherein said Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K.

7. The computer-readable medium as recited in Claim 5, wherein determining said Squared Tate pairing further includes:

forming a mathematical chain for m, wherein m is a positive integer and an m-torsion element D is fixed on Jacobian of said hyperelliptic curve C.

8. The computer-readable medium as recited in Claim 7, wherein said mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain.

9. An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process;

logic operatively coupled to said memory and configured to calculate at least one Squared Tate pairing for at least one hyperelliptic curve, and at least partially support cryptographic processing of selected stored information based on said determined Squared Tate pairing.

10. The apparatus as recited in Claim 9, wherein said Squared Tate pairing is defined for at least one hyperelliptic curve C of genus g over a field K.

11. The apparatus as recited in Claim 9, wherein said logic is further configured to form a mathematical chain for m, wherein m is a positive integer and an m-torsion element D is fixed on Jacobian of said hyperelliptic curve C.

12. The apparatus as recited in Claim 11, wherein said mathematical chain includes a mathematical chain selected from a group of mathematical chains comprising an addition chain and an addition-subtraction chain.

13. A method comprising:

determining a hyperelliptic curve C of genus g over a field K and a positive integer m;

determining a Jacobian $J(C)$ of said hyperelliptic curve C, and wherein each element D of $J(C)$ contains a representative of the form $A - g(\boldsymbol{P}_0)$, where A is an effective divisor of degree g; and

determining a plurality of functions $h_{j,D}$ that are iterative building blocks for the formation of a function $h_{m,D}$ in order to evaluate v_m which is a Squared Tate pairing.

14. The method as recited in Claim 13, wherein said hyperelliptic curve C is over a field not of characteristic 2.

15. The method as recited in Claim 13, wherein

for at least one element D of $J(C)$, a representative for iD will be $A_i - g(\boldsymbol{P}_0)$, where A_i is effective of degree g.

16. The method as recited in Claim 13, wherein if $P=(x, y)$ is a point on said hyperelliptic curve C, then $\boldsymbol{-P}$ denotes a point $\boldsymbol{-P}:=(x, -y)$, and wherein if a point $P=(x, y)$ occurs in A and $y \neq 0$, then $\boldsymbol{-P} := (x,-y)$ does not occur in A and a representative for identity will be $g(\boldsymbol{P}_0)$.

17. The method as recited in Claim 16, further comprising:

to a representative A_i, associating two polynomials (a_i, b_i) which represent a divisor.

18. The method as recited in Claim 16, further comprising:

determining D as an m-torsion element of $J(C)$.

19. The method as recited in Claim 18, further comprising:

if j is an integer, then $h_{j,D} = h_{j,D}(X)$ denoting a rational function on C with divisor $(h_{j,D}) = jA_1 - A_j - ((j-1)\, g)\, (\boldsymbol{P}_0)$.

20. The method as recited in Claim 18, wherein D is an m-torsion divisor and $A_m = g(\boldsymbol{P}_0)$, and a divisor of $h_{m,D}$ is $(h_{m,D}) = mA_1 - mg(\boldsymbol{P}_0)$.

21 The method as recited in Claim 18, wherein $h_{m,D}$ is well-defined up to a multiplicative constant.

22. The method as recited in Claim 18, further comprising:

evaluating $h_{m,D}$ at a degree zero divisor E on said hyperelliptic curve C, wherein E does not contain $\boldsymbol{P}_0$ and E is prime to A_i.

23. The method as recited in Claim 18, wherein E is prime to A_i for all i in an addition-subtraction chain for m.

24. The method as recited in Claim 22, wherein given A_i, A_j, and A_{i+j}, further comprising determining a function $u_{i,j}$ such that a divisor of $u_{i,j}$ is $(u_{i,j}) = A_i + A_j - A_{i+j} - g(\boldsymbol{P}_0)$.

25. The method as recited in Claim 22, further comprising:

evaluating $h_{j,D}(E)$ such that when j=1, $h_{1,D}$ is 1.

26. The method as recited in Claim 22, further comprising:

given A_i, A_j, $h_{i,D}(E)$ and $h_{j,D}(E)$, evaluating $u_{i,j}$ to be $(u_{i,j})=A_i + A_j - A_{i+j} - g(\boldsymbol{P}_0)$, and $h_{i+j,D}(E)= h_{i,D}(E)\ h_{j,D}(E)\ u_{i,j}\ (E)$.

27. The method as recited in Claim 13, further comprising:

determining a function $(u_{i,j}) = A_i + A_j - A_{i+j} - g(\boldsymbol{P}_0)$.

28. The method as recited in Claim 27, wherein $g = 2$ and

$(u_{i,j}) = A_i + A_j - A_{i+j} - 2(\boldsymbol{P}_0)$ is determined as follows

$u_{i,j}(\boldsymbol{X}) := \dfrac{a_{\text{new}}(x(\boldsymbol{X}))}{b_{\text{new}}(x(\boldsymbol{X})) + y(\boldsymbol{X})} * d(x(\boldsymbol{X}))$, if the degree of a_{new} is greater than 2, otherwise, $u_{i,j}$ is determined as $u_{i,j}\ (\boldsymbol{X}) := d(x(\boldsymbol{X}))$, wherein $d(x)$ is the greatest common divisor of three polynomials $(a_i(x), a_j(x), b_i(x)+b_j(x))$.

29. The method as recited in Claim 13, further comprising:

determining a Squared Tate pairing for a hyperelliptic curves v_m, for an m-torsion element D of a Jacobian $J(C)$ and an element E of $J(C)$, with representatives $(\boldsymbol{P}_1)+(\boldsymbol{P}_2)+\ldots+(\boldsymbol{P}_g) - g(\boldsymbol{P}_0)$ and $(\boldsymbol{Q}_1)+(\boldsymbol{Q}_2)+\ldots+(\boldsymbol{Q}_g) - g(\boldsymbol{P}_0)$,

respectively, with each $\boldsymbol{P}_i$ and each $\boldsymbol{Q}_j$ on the curve C, with $\boldsymbol{P}_i$ not equal to $\pm\boldsymbol{Q}_j$ for all i, j, determining that

$$v_m(D,E) := (h_{m,D}((\boldsymbol{Q}_1)-(-\boldsymbol{Q}_1)+(\boldsymbol{Q}_2)-(-\boldsymbol{Q}_2)+\ldots+(\boldsymbol{Q}_g)-(-\boldsymbol{Q}_g))^{\frac{q-1}{m}}.$$

30. A computer-readable medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

determining a hyperelliptic curve C of genus g over a field K and a positive integer m;

determining a Jacobian $J(C)$ of said hyperelliptic curve C, and wherein each element D of $J(C)$ contains a representative of the form $A - g(\boldsymbol{P}_0)$, where A is an effective divisor of degree g; and

determining a plurality of functions $h_{j,D}$ that are iterative building blocks for the formation of a function $h_{m,D}$ in order to evaluate v_m which is a Squared Tate pairing.

31. The computer-readable medium as recited in Claim 30, wherein said hyperelliptic curve C is not of characteristic 2.

32. The computer-readable medium as recited in Claim 30, wherein

for at least one element D of $J(C)$, a representative for iD will be $A_i - g(\boldsymbol{P}_0)$, where A_i is effective of degree g.

33. The computer-readable medium as recited in Claim 30, wherein if $P=(x, y)$ is a point on said hyperelliptic curve C, then $-\boldsymbol{P}$ denotes a point $-\boldsymbol{P}:=(x,$

$-y$), and wherein if a point $P=(x, y)$ occurs in A and $y \neq 0$, then $\boldsymbol{-P} := (x,-y)$ does not occur in A and a representative for identity will be $g(\boldsymbol{P}_0)$.

34. The computer-readable medium as recited in Claim 33, further comprising:

to a representative A_i, associating two polynomials (a_i, b_i) which represent a divisor.

35. The computer-readable medium as recited in Claim 33, further comprising:

determining D as an m-torsion element of $J(C)$.

36. The computer-readable medium as recited in Claim 35, further comprising:

if j is an integer, then $h_{j,D} = h_{j,D}(X)$ denoting a rational function on C with divisor $(h_{j,D}) = jA_1 - A_j - ((j-1)\, g)\, (\boldsymbol{P}_0)$.

37. The computer-readable medium as recited in Claim 35, wherein D is an m-torsion divisor and $A_m = g(\boldsymbol{P}_0)$, and a divisor of $h_{m,D}$ is $(h_{m,D}) = mA_1 - mg(\boldsymbol{P}_0)$.

38 The computer-readable medium as recited in Claim 35, wherein $h_{m,D}$ is well-defined up to a multiplicative constant.

39. The computer-readable medium as recited in Claim 35, further comprising:

evaluating $h_{m,D}$ at a degree zero divisor E on said hyperelliptic curve C, wherein E does not contain P_0 and E is prime to A_i.

40. The computer-readable medium as recited in Claim 35, wherein E is prime to A_i for all i in an addition-subtraction chain for m.

41. The computer-readable medium as recited in Claim 39, wherein given A_i, A_j, and A_{i+j}, further comprising determining a function $u_{i,j}$ such that a divisor of $u_{i,j}$ is $(u_{i,j}) = A_i + A_j - A_{i+j} - g(\boldsymbol{P}_0)$.

42. The computer-readable medium as recited in Claim 39, further comprising:

evaluating $h_{j,D}(E)$ such that when j=1, $h_{1,D}$ is 1.

43. The computer-readable medium as recited in Claim 39, further comprising:

given A_i, A_j, $h_{i,D}(E)$ and $h_{j,D}(E)$, evaluating $u_{i,j}$ to be $(u_{i,j})$=$A_i + A_j - A_{i+j} - g(\boldsymbol{P}_0)$,, and $h_{i+j,D}(E)$= $h_{i,D}(E)$ $h_{j,D}(E)$ $u_{i,j}$ (E).

44. The computer-readable medium as recited in Claim 30, further comprising:

determining a function $(u_{i,j}) = A_i + A_j - A_{i+j} - g(\boldsymbol{P}_0)$.

45. The computer-readable medium as recited in Claim 44, wherein g = 2 and

$(u_{i,j}) = A_i + A_j - A_{i+j} - 2(\boldsymbol{P}_0)$ is determined as follows

$u_{i,j}(\boldsymbol{X}) := \dfrac{a_{\text{new}}(x(\boldsymbol{X}))}{b_{\text{new}}(x(\boldsymbol{X})) + y(\boldsymbol{X})} * d(x(\boldsymbol{X}))$, if the degree of a_{new} is greater than 2, otherwise, $u_{i,j}$ is determined as $u_{i,j}$ $(\boldsymbol{X}) := d(x(\boldsymbol{X}))$, wherein $d(x)$ is the greatest common divisor of three polynomials $(a_i(x), a_j(x), b_i(x)+b_j(x))$.

46. The computer-readable medium as recited in Claim 30, further comprising:

determining a Squared Tate pairing for a hyperelliptic curves v_m, for an m-torsion element D of a Jacobian $J(C)$ and an element E of $J(C)$, with representatives $(\boldsymbol{P}_1)+(\boldsymbol{P}_2)+\ldots+(\boldsymbol{P}_g) - g(\boldsymbol{P}_0)$ and $(\boldsymbol{Q}_1)+(\boldsymbol{Q}_2)+\ldots+(\boldsymbol{Q}_g) - g(\boldsymbol{P}_0)$, respectively, with each $\boldsymbol{P}_i$ and each $\boldsymbol{Q}_j$ on the curve C, with $\boldsymbol{P}_i$ not equal to $\pm\boldsymbol{Q}_j$ for all i, j, determining that

$$v_m(D,E) := (h_{m,D}\left((\boldsymbol{Q}_1)-(-\boldsymbol{Q}_1)+(\boldsymbol{Q}_2)-(-\boldsymbol{Q}_2)+\ldots+(\boldsymbol{Q}_g)-(-\boldsymbol{Q}_g)\right)^{\frac{q-1}{m}}.$$

47. An apparatus comprising:

memory configured to store information suitable for use with using a cryptographic process; and

logic operatively coupled to said memory and configured to determine a hyperelliptic curve C of genus g over a field K and a positive integer m, determine a Jacobian $J(C)$ of said hyperelliptic curve C, wherein each element D of $J(C)$ contains a representative of the form $A - g(\boldsymbol{P}_0)$ and A is an effective divisor of degree g, and determine a plurality of functions $h_{j,D}$ that are iterative building blocks for the formation of a function $h_{m,D}$ in order to evaluate v_m which is a Squared Tate pairing.

48. The apparatus as recited in Claim 47, wherein said hyperelliptic curve C is not of characteristic 2.

49. The apparatus as recited in Claim 47, wherein

for at least one element D of $J(C)$, a representative for iD will be $A_i - g(\boldsymbol{P}_0)$, where A_i is effective of degree g.

50. The apparatus as recited in Claim 47, wherein if $P=(x, y)$ is a point on said hyperelliptic curve C, then $-\boldsymbol{P}$ denotes a point $-\boldsymbol{P}:=(x, -y)$, and wherein if a point $P=(x, y)$ occurs in A and $y \neq 0$, then $-\boldsymbol{P} := (x,-y)$ does not occur in A and a representative for identity will be $g(\boldsymbol{P}_0)$.

51. The apparatus as recited in Claim 50, wherein said logic is further configured to, for a representative A_i, associate two polynomials (a_i, b_i) which represent a divisor.

52. The apparatus as recited in Claim 50, wherein said logic is further configured to determine D as an m-torsion element of $J(C)$.

53. The apparatus as recited in Claim 52, wherein said logic is further configured to, if j is an integer, then determine $h_{j,D} = h_{j,D}(X)$ by denoting a rational function on C with divisor $(h_{j,D}) = jA_1 - A_j - ((j-1)\,g)\,(\boldsymbol{P}_0)$.

54. The computer-readable medium as recited in Claim 52, wherein D is an m-torsion divisor and $A_m = g(\boldsymbol{P}_0)$, and a divisor of $h_{m,D}$ is $(h_{m,D}) = mA_1 - mg(\boldsymbol{P}_0)$.

55 The apparatus as recited in Claim 52, wherein $h_{m,D}$ is well-defined up to a multiplicative constant.

56. The apparatus as recited in Claim 52, wherein said logic is further configured to evaluate $h_{m,D}$ at a degree zero divisor E on said hyperelliptic curve C, wherein E does not contain $\boldsymbol{P}_0$ and E is prime to A_i.

57. The apparatus as recited in Claim 52, wherein E is prime to A_i for all i in an addition-subtraction chain for m.

58. The apparatus as recited in Claim 56, wherein given A_i, A_j, and A_{i+j}, and wherein said logic is further configured to determine a function $u_{i,j}$ such that a divisor of $u_{i,j}$ is $(u_{i,j}) = A_i + A_j - A_{i+j} - g(\boldsymbol{P}_0)$.

59. The apparatus as recited in Claim 56, wherein said logic is further configured to evaluate $h_{j,D}(E)$ such that when j=1, $h_{1,D}$ is 1.

60. The apparatus as recited in Claim 56, wherein said logic is further configured to, given A_i, A_j, $h_{i,D}(E)$ and $h_{j,D}(E)$, evaluate $u_{i,j}$ to be $(u_{i,j})=A_i + A_j - A_{i+j} - g(\boldsymbol{P}_0)$,, and $h_{i+j,D}(E)= h_{i,D}(E)\ h_{j,D}(E)\ u_{i,j}\ (E)$.

61. The apparatus as recited in Claim 47, wherein said logic is further configured to determine a function $(u_{i,j}) = A_i + A_j - A_{i+j} - g(\boldsymbol{P}_0)$.

62. The apparatus as recited in Claim 61, wherein $g = 2$ and

$(u_{i,j}) = A_i + A_j - A_{i+j} - 2(\boldsymbol{P}_0)$ is determined by said logic as follows

$u_{i,j}(\boldsymbol{X}) := \dfrac{a_{\text{new}}(x(\boldsymbol{X}))}{b_{\text{new}}(x(\boldsymbol{X})) + y(\boldsymbol{X})} * d(x(\boldsymbol{X}))$, if the degree of a_{new} is greater than 2, otherwise, $u_{i,j}$ is determined as $u_{i,j}\ (\boldsymbol{X}) := d(x(\boldsymbol{X}))$, wherein $d(x)$ is the greatest common divisor of three polynomials $(a_i(x), a_j(x), b_i(x)+b_j(x))$.

63. The apparatus as recited in Claim 47, wherein said logic is further configured to determine a Squared Tate pairing for a hyperelliptic curves v_m, for an m-torsion element D of a Jacobian $J(C)$ and an element E of $J(C)$, with representatives $(\boldsymbol{P}_1)+(\boldsymbol{P}_2)+\ldots+(\boldsymbol{P}_g) - g(\boldsymbol{P}_0)$ and $(\boldsymbol{Q}_1)+(\boldsymbol{Q}_2)+\ldots+(\boldsymbol{Q}_g) - g(\boldsymbol{P}_0)$, respectively, with each $\boldsymbol{P}_i$ and each $\boldsymbol{Q}_j$ on the curve C, with $\boldsymbol{P}_i$ not equal to $\pm\boldsymbol{Q}_j$ for all i, j, and to determine that

$$v_m(D,E) := (h_{m,D}\left((\boldsymbol{Q}_1)-(-\boldsymbol{Q}_1)+(\boldsymbol{Q}_2)-(-\boldsymbol{Q}_2)+\ldots+(\boldsymbol{Q}_g)-(-\boldsymbol{Q}_g)\right)^{\frac{q-1}{m}}.$$